In the Claims:

Please amend Claims 1, 2, 3, 7, 8, 10, 11, 16, 17, 19 and 20, all as shown below. Applicant respectfully reserves the right to prosecute any originally presented or canceled claims in a continuing or future application.

1.   (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

   (1) a policy manager, coupled to a network, including

      a database for storing a security policy including a plurality of rules; and

      a policy distributor, coupled to the database, for distributing the plurality of rules through the network;

   (2) a security engine located on a client coupled to the network, for storing a set of the plurality of rules constituting a local customized security policy received through the network from the policy distributor, and for enforcing the rules local customized security policy with respect to an application at the client; and

   (3) an application, coupled to the security engine.

2.   (Currently Amended) The system of claim 1, wherein the rules are stored separate from the application rather than being embedded in the application.

3.   (Currently Amended) The system of claim 1, wherein the security engine further comprises:

   an engine for, based on the rules, evaluating a request to access the application based on the set of the plurality of rules; and

   an application programming interface (API) for enabling the application and the engine to communicate.

4.   (Original) The system of claim 3, wherein the security engine further comprises: a plug-in application programming interface (API) for extending capabilities of the security engine.

- 4 -

5.   (Original) The system of claim 1, further comprising: location means for enabling components in the system to locate each other through the network.

6.   (Original) The system of claim 1, wherein the policy manager and the policy distributor are hosted on a first server, the security engine and the application are hosted on a second server, and the first and second servers are communicatively coupled to each other through the network.

7.   (Currently Amended) A system for maintaining security for an application in a distributed computing environment, comprising:

an engine located at a client coupled to a network, for storing a set of rules constituting a local customized policy received through the network from a centralized location, and for enforcing the rules local customized policy at an application level of the client;

an interface coupled to the engine for evaluating the local customized policy in order to control access to an application at the client; and

an application, coupled to the interface to enable the application so as to communicate with the engine.

8.   (Currently Amended) The system of claim 7, wherein the engine stores the rules separate from the application rather than being embedded in the application.

9.   (Original) The system of claim 7, further comprising: a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

10.   (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including

a database for storing a security policy including a plurality of rules; and

a policy distributor for distributing <u>a set of</u> the <u>plurality of</u> rules through the network <u>to a receiving component wherein the distributed set of rules represents a local customized security policy for that receiving component</u>;

(2) a plurality of security engines, <u>each located at the receiving component</u> coupled to the network, for receiving a set of <u>the plurality of</u> rules through the network from the policy distributor, storing the set of rules, and enforcing <u>the local customized security policy by evaluating</u> the set of rules; and

(3) a plurality of applications, each application being coupled to ~~a respective~~ <u>one of the plurality of</u> security ~~engine~~ <u>engines, each</u> <u>the</u> security engine being able to enforce a set of rules for ~~its respective~~ <u>the</u> application <u>coupled to it</u>.

11. (Currently Amended) ~~A~~ <u>The</u> system of claim 10, wherein the security engines store the rules separate from each application <u>rather than being embedded in the application.</u>

12. (Original) The system of claim 10, wherein each security engine further comprises:
an engine for, based on a set of rules, evaluating a request to access a particular application; and
an application programming interface (API) for enabling a respective application to communicate with a respective engine.

13. (Original) The system of claim 12, wherein each security engine further comprises: a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

14. (Original) The system of claim 10, further comprising: location means for enabling components in the system to locate each other through the network.

15. (Original) The system of claim 10, wherein the policy manager and the policy distributor are hosted on a policy server, the plurality of security engines and the plurality of applications are hosted

on at least one separate server, and the policy server is communicatively couples through the network to the separate server.

16.   (Currently Amended) A system for maintaining security for a plurality of applications in a distributed computing environment, comprising:

an engine located at a client coupled to a network, for storing a set of rules constituting a local security policy customized for the client, wherein the set of rules is received through the network from a centralized location, and for enforcing the wherein the local security policy is enforced by the engine by evaluating the set of rules;

a plurality of interfaces coupled to the engine; and

a plurality of applications, each application being coupled to a respective interface one of the plurality of interfaces to enable the application to communicate with the engine through its respective interface the one of the plurality of interfaces, wherein the engines enforcing the rules engine enforces the local security policy for the application.

17.   (Currently Amended) The system of claim 16, wherein the rules are stored separate from each application rather than being embedded in the application.

18.   (Original) The system of claim 17, further comprising: a plug-in application programming interface (plug-in API) for extending capabilities of the engine.

19.   (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

a policy manager including a policy database for storing a security policy having a plurality of rules;

zero one or more security engines for storing and enforcing a set of the plurality of rules with respect to an application, said policy manager and said zero one or more security engines residing on a single server; and

- 7 -

an application, coupled to the ~~zero~~ <u>one</u> or more security engines;

wherein updates to the security policies residing on other servers may be synchronized through database replication;

<u>wherein the policy manager is capable of distributing a custom local security policy to other servers on the network for enforcement thereof by the security engine located on each of the other servers.</u>

20.   (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

a policy manager including a policy database for storing a security policy having a plurality of rules;

~~zero~~ <u>one</u> or more security engines for storing and enforcing a set of <u>the plurality of</u> rules with respect to an application, said policy manager and said ~~zero~~ <u>one</u> or more security engines residing on a central server; and

an application coupled to the ~~zero~~ <u>one</u> or more security engines;

wherein other servers storing local security policies may, in response to an authorization request, synchronize local security policy updates with the central server; <u>and</u>

<u>wherein the policy manager is capable of distributing a custom local security policy to other servers on the network for enforcement thereof by the security engine located on each of the other servers.</u>